международным стандартам интерфейса с различными базами данных визуализации связей и обмена аналитической информацией.

Список литературы

1. URL: http://www.e-biblio.ru/book/bib/01_informatika/IAS/Book.html
2. URL: http://itdirector.org.ua/club/My_forum/forum10/topic19/
3. URL: http://life-prog.ru/1_759_OLTP — i-OLAP-tehnologii.html

УДК 654.072.7

С. С. Блинов
Научный руководитель: ст. преп. В. В. Шкитенков
Уральский федеральный университет, Екатеринбург

ИДЕНТИФИКАЦИЯ БАЗОВЫХ СТАНЦИЙ ОПЕРАТОРОВ СОТОВОЙ СВЯЗИ С ПОМОЩЬЮ ПОРТАТИВНОГО КОМПЛЕКСА РАДИОКОНТРОЛЯ

Аннотация. В статье рассматривается проблема незаконного использования радиочастотного ресурса и алгоритмы идентификации базовых станций, эксплуатируемых операторами сотовой связи с нарушением законодательства Российской Федерации.

Ключевые слова: базовая станция; GSM; UMTS; LTE аппаратно-программный комплекс; радиоэлектронная обстановка; радиоконтроль; сотовая связь.

На 2017 год Роскомнадзором было выявлено более 13000 базовых станций, установленных с нарушением законов РФ [1] или не имеющих разрешения на использование частот. Для выявления таких базовых станций Радиочастноным центром проводятся периодические мероприятия радиоконтроля. Для анализа и контроля радиоэлектронной обстановки используются мобильные комплексы радиоконтроля. Всех их объединяют большие габариты и огромная стоимость — более 10 млн рублей за одно устройство. Это обусловлено тем, что для использования таких комплексов требуется переоборудование дорогих автомобилей, таких как Ford Transit или Toyota Land Cruiser, а для питания комплексов требуются мощные дизель-генераторы [2].

Следовательно, можно сформулировать цель — разработка портативного устройства для измерение радиоэлектронной обстановки в сетях сотовой связи стандартов GSM, UMTS и LTE, которое будет значительно дешевле и компактнее ныне существующих.

При помощи действующих комплексов осуществлять радиоконтроль в помещениях невозможно. Более того, такие комплексы имеют намного больший функционал и избыточную точность для решения поставленной задачи.

В процессе работы проведен обзор существующих мобильных комплексов измерений РЭО, а также составлена концепция разрабатываемого устройства под требуемые функциональные возможности.

В результате работы разработан готовый аппаратно-программный комплекс измерений РЭО в сетях радиосвязи стандарта GSM, UMTS и LTE, включающий в себя аппаратную часть, выполненную в виде моноблока с возможностью подключения внешней антенны [3] и программную часть с возможностями декодирования системной информации РЭС базовых станций стандартов беспроводной связи GSM, UMTS и LTE по результатам измерений РЭО, извлечение координатной информации с приемника GPS [4] по маршруту передвижения комплекса, вывода информации в графический интерфейс пользователя (переносная ЭВМ), отображения электронной карты местности в режиме офлайн (без подключения к сети Интернет) и формирования итогового отчета «Контроль загруженности частот» для постобработки модулем оценки местоположения. В дальнейшем по этому отчету производится сверка с базой данных на предмет наличия или отсутствия конкретной базовой станции в этой базе.

Аппаратная часть выполнена в виде компактного переносного моноблока (габариты (Д × Ш × В) 190 × 140 × 80 мм и масса 680 г). В качестве телекоммуникационного модуля использован SIM7100E от компании SIMCom [5], в качестве питания использован встроенный аккумулятор, но поддерживается и внешние источники 5 В, 2 А. Имеется возможность использования внешних направленных и ненаправленных антенн для повышения точности и разнесенного приема.

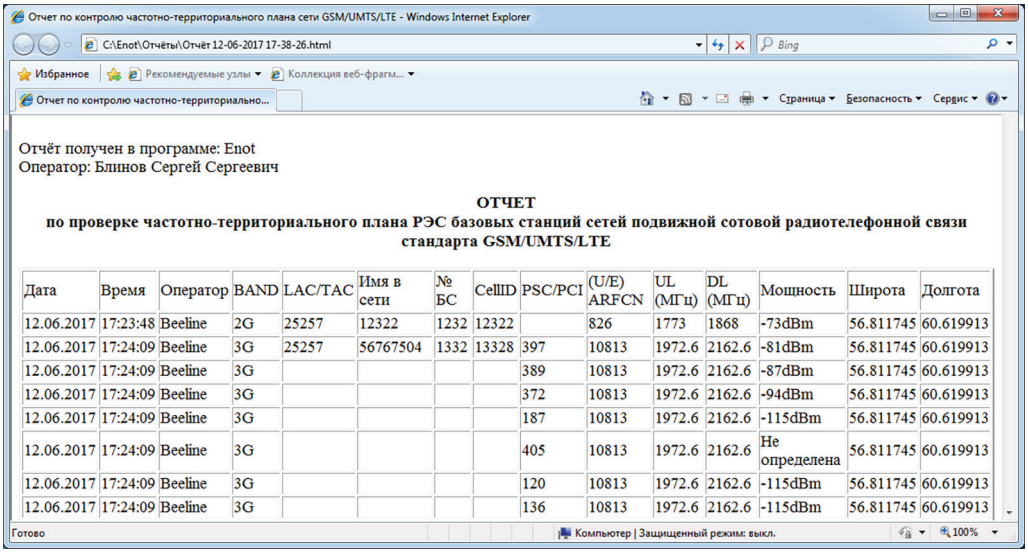
ПО разработано в Qt Creator с использованием кроссплатформенной библиотеки Qt 5.7.1 и компилятора MSVC2015. Распространяется в виде одного установочного файла.

Фотографию готового устройства можно увидеть на рис. 1 слева, а его наполнение — на рис. 1 справа. Скриншот сформированного отчета в формате HTML продемонстрирован на рис. 2.

За счет того, что в основе аппаратной части использован модуль SIM7100E, имеется возможность в дальнейшем реализовать работу не только с одним оператором, но и с несколькими одновременно, а также получать еще больше системной информации при необходимости. При этом за счет того, что ПО разработано в виде функций, в дальнейшем возможно как развитие уже разработанных функций, так и добавление новых, а благодаря использованию кроссплатформенной библиотеки Qt и отказа от использования Windows API,

возможна сборка проекта под различные операционные системы, в том числе под операционные системы одноплатных компьютеров.

Рис. 1. Общий вид устройства (слева) и его наполнение (справа)



Отчёт по контролю частотно-территориального плана сети GSM/UMTS/LTE - Windows Internet Explorer

C:\Enot\Отчёты\Отчёт 12-06-2017 17-38-26.html

Отчёт получен в программе: Enot
Оператор: Блинов Сергей Сергеевич

ОТЧЕТ
по проверке частотно-территориального плана РЭС базовых станций сетей подвижной сотовой радиотелефонной связи стандарта GSM/UMTS/LTE

Дата	Время	Оператор	BAND	LAC/TAC	Имя в сети	№ БС	CellID	PSC/PCI	(U/E) ARFCN	UL (МГц)	DL (МГц)	Мощность	Широта	Долгота
12.06.2017	17:23:48	Beeline	2G	25257	12322	1232	12322		826	1773	1868	-73dBm	56.811745	60.619913
12.06.2017	17:24:09	Beeline	3G	25257	56767504	1332	13328	397	10813	1972.6	2162.6	-81dBm	56.811745	60.619913
12.06.2017	17:24:09	Beeline	3G					389	10813	1972.6	2162.6	-87dBm	56.811745	60.619913
12.06.2017	17:24:09	Beeline	3G					372	10813	1972.6	2162.6	-94dBm	56.811745	60.619913
12.06.2017	17:24:09	Beeline	3G					187	10813	1972.6	2162.6	-115dBm	56.811745	60.619913
12.06.2017	17:24:09	Beeline	3G					405	10813	1972.6	2162.6	Не определена	56.811745	60.619913
12.06.2017	17:24:09	Beeline	3G					120	10813	1972.6	2162.6	-115dBm	56.811745	60.619913
12.06.2017	17:24:09	Beeline	3G					136	10813	1972.6	2162.6	-115dBm	56.811745	60.619913

Готово | Компьютер | Защищенный режим: выкл. | 100%

Рис. 2. Отчет в формате HTML

В качестве заключения стоит отметить, что устройство в данный момент работает исправно и используется по назначению. Также ведутся работы над значительным расширением функционала и снижением габаритов и массы.

Список литературы

1. В России на 55 % выросло количество базовых станций стандарта LTE [Электронный ресурс]. Режим доступа: http://rkn.gov.ru/news/rsoc/news43427.htm (дата обращения: 10.11.2017).

2. Каталог ИРКОС. Автоматизированные системы и технические средства радиоконтроля, 2017. 122 с.

3. *Соловьянова И. П.*, *Наймушин М. П.* Теория волновых процессов. Электромагнитные волны : учеб. пособие. Екатеринбург : ГОУ ВПО УГТУ–УПИ, 2005. 131 с.

4. SIM7100 GPS Application Note/ Shanghai SIMCom Wireless Solutions Ltd., 2015. 13 с.

5. SIM7100 Series Hardware Design V1.09 / Shanghai SIMCom Wireless Solutions Ltd., 2017. 66 с.

УДК 004.056.53

И. А. Бойко, К. Л. Стойчин
Научный руководитель: д-р тех. наук, проф. С. В. Поршнев
Уральский федеральный университет, Екатеринбург

ПРОБЛЕМА СОВРЕМЕННЫХ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Аннотация. В настоящей статье рассмотрены проблемы современных методов социальной инженерии. Данное исследование имеет цель рассмотреть методику работы людей, владеющих навыками социальной инженерии. Результатами данной работы являются рекомендации, помогающие предотвратить утечку информации людям, владеющими навыками социальной инженерии.

Ключевые слова: социальная инженерия; VPN; схема; лицо; владеющее методами социальной инженерии.

В современном мире большую ценность имеет такой ресурс, как информация. Она имеет ценность для человека или предприятия, которые владеют ею. Несложно догадаться, что в случае утечки ценной информации владельцу будет нанесен ущерб, который в большинстве случаев принесет материальные убытки, а также изменит нормальный ритм работы персонала. Для сохранности ценной информации в тайне разрабатываются различные программные и аппаратные средства защиты информации, позволяющие минимизировать шансы ее утечки с системы электронно-вычислительных устройств. Но как бы надежно ни была защищена система, главной уязвимостью в утечке защищенной информации является человек. Он является слабым звеном в системе защиты информации. При правильном подходе злоумышленника посвященный человек способен выдать ему всю защищенную информацию, которую он потребует. Такой подход к получению защищенной информации имеет название